Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1 (Currently Amended). A method of protecting a ~~document~~ check, which will be transformed into a value bearing instrument after adding additional markings to the ~~document~~ check, from fraudulent alteration of the markings comprising the steps of:

generating encryptions of a unique identifier X of the document, the unique identifier X being check data including a bank ID, an account ID number and a check number printed on the ~~document~~ check, the encryptions being $\mathrm{Sign}_{k,0}(X)$, where $\mathrm{Sign}_{k,0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the check, $\mathrm{Sign}_{k,0}(X)$ being used to authenticate the check; and

covering each critical field k, k=1,2,3..., of the ~~document~~ check where markings are to be added with ~~encrypted versions of X $\mathrm{Sign}_{k,0}(X)$, where $\mathrm{Sign}_{k,0}(X)$ is a family of cryptographic functions which is known only to an institution which issues the document, $\mathrm{Sign}_{k,0}(X)$ being used to authenticate the document~~ a large number of lines of fine print, the lines of fine print comprising the cryptographic function Sign_k, the critical fields k including a date field, a payee field, amount fields, a payer's signature field, and an endorser's field.

2 (Canceled).

3 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim ~~2~~ 1, wherein each critical field k of the document, in addition to being covered by the encrypted version of X, $\mathrm{Sign}_{k,0}(X)$, is covered with another encrypted version of X, $\mathrm{Sign}_k(X)$, where $\mathrm{Sign}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial

authentication of the ~~document~~ check.

4 (Canceled).

5 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 3, wherein each critical field k of the ~~document~~ check, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_k(X)$ and $\mathrm{Sign}_{k,0}(X)$, is covered with a third encrypted version of X, $\mathrm{Sec}_k(X)$, where $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$ which is known to a small group within the institution which issues the ~~document~~ check for performing final authentication of the ~~document~~ check.

6 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 5, further comprising the step of indexing the cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k, by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $\mathrm{Sign}_k(X)$, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sec}_k(X)$ is a family of different cryptographic functions.

7 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 6, wherein the families of cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k prevent cryptographic functions which have been obscured at different places by marks added to the ~~document~~ check from being used to reconstitute the full cryptographic function.

8 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 1, wherein electronic deposit of a ~~document~~ check transformed into a value bearing instrument comprises the steps of:

scanning the ~~document~~ check with a scanner to generate a digitized version of the ~~document~~ check ; and

transmitting the digitized version of the ~~document~~ check for deposit.

9 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 8, wherein electronic deposit of a ~~document~~ check transformed into a value bearing instrument further comprises the step of endorsing the ~~document~~ check, if needed, having printed thereon encryptions in at least selected locations where markings are added to transform the ~~document~~ check into a value bearing instrument, the act of endorsing obscuring some of the encryptions.

10 (Currently Amended).The method of protecting a ~~document~~ check from fraudulent alteration recited in claim ~~8~~ 5, wherein electronic deposit of a ~~document~~ transformed into a value bearing instrument further comprises the steps of:

generating a digitized version of the check in at least selected locations where markings are added to transform the check into a value bearing instrument;

extracting from the digitized version of the ~~document~~ check the unique identifier X and a corresponding digital encryption of X, Sign$_k$(X), which is known to a large number of authorized institutions; and

comparing a decrypted version of Sign$_k$(X) to the unique identifier X as an initial authentication of the ~~document~~ check.

11 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 10, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the ~~document~~ check the unique identifier X and a corresponding digital encryption of X, Sign$_{k,0}$(X), which is known only to an institution that issues the ~~document~~ check; and comparing a decrypted version of Sign$_{k,0}$(X) to the unique identifier X as a further authentication of the ~~document~~ check.

12 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 11, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the ~~document~~ check the unique identifier X and a corresponding digital encryption of X, Sec$_k$(X), which is known to a small group within the institution that issues the ~~document~~ check; and

comparing a decrypted version of Sec$_k$(X) to the unique identifier X as a final authentication of the ~~document~~ check.

13 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 1, wherein portions of the lines of fine print are obscured by writing added to the ~~document~~ check when transforming the ~~document~~ check into a value bearing instrument.

14 (Canceled).

15 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim ~~14~~ 1, wherein an issuing bank chooses a first secret key Sign$_k$ using a secure cryptographic generator (SCG), further comprising the steps of:

computing ~~a~~ the first family of encrypted functions Sign$_k$(X); and

communicating the key Sign$_k$ to banks and other authorized institutions involved in depositing of checks, the family of encrypted functions Sign$_k$(X) allowing the payee's bank to perform a first authentication of the check.

16 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 15, wherein an issuing bank chooses a second secret key $Sign_{k,0}$ using a SCG, further comprising the steps of:

computing ~~a~~ the second family of encrypted functions $Sign_{k,0}(X)$, key $Sign_{k,0}$ remaining the exclusive property of the issuing bank; and

using SCGs, communicating the key $Sign_{k,0}$ to all branches of the issuing bank where check clearing is done, the family of encrypted functions $Sign_{k,0}(X)$ being used exclusively by the issuing bank and branches involved in the clearing of checks.

17 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 16, wherein an issuing bank chooses a third secret key Sec_k which is exclusively known to a small group within the issuing bank, further comprising the step of computing ~~a~~ the third family of encrypted functions $Sec_k(X)$, the secret key Sec_k being used by the issuing bank as final instrument to verify the check.

18 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim ~~14~~ 1, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) .

19 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim ~~14~~ 5, wherein electronic deposit of the check by a payee comprises the steps of:

endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions;

scanning the endorsed check with a scanner to generate a digitized version of the check;

transmitting the digitized version of the check for deposit to the payee's bank.

20 (Currently Amended).The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 19, wherein electronic deposit of the check by a payee comprises the steps of:

extracting by the payee's bank from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\text{Sign}_k(X)$, which is known to a large number of authorized institutions including the payee's bank; and

comparing by the payee's bank a decrypted version of $\text{Sign}_k(X)$ to the unique identifier X as an initial authentication of the check.

21 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 20, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\text{Sign}_{k,0}(X)$, which is known only to a bank that issues the check; and

comparing by the payor's bank a decrypted version of $\text{Sign}_{k,0}(X)$ to the unique identifier X as a further authentication of the check.

22 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 21, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\text{Sec}_k(X)$, which is known to a small group within the bank that issues the check; and

comparing a decrypted version of $\text{Sec}_k(X)$ to the unique identifier X as a final authentication of the check.

23 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 19, further comprising the step

of accessing a database by the payee's bank where the unique identifier X and first encrypted function $\mathrm{Sign}_k(X)$ is registered to determine whether the check has been previously presented for deposit.

24 (Currently Amended). The method of protecting a ~~document~~ check from fraudulent alteration recited in claim 19, further comprising the step of registering a check to be deposited by the payee with ~~an~~ a secure cryptgraphic generator (SCG) to prevent multiple deposits.

25 (Currently Amended). A ~~document~~ check protecting against fraudulent alteration of markings added to the ~~document~~ check to transform the ~~document~~ check into a value bearing instrument, the ~~document~~ check having printed thereon a unique identifier X, the unique identifier including a bank ID, an account ID number and a check number, the check further having critical fields k, k=1,2,3..., the critical fields including a date field, a payee field, amount fields, a payer's field, and an endorser's field, and ~~covering~~ each critical field k, k=1,2,3..., being covered a large number of lines of fine print comprising ~~where markings are added to the document~~ encrypted versions ~~a~~ the unique identifier X printed on the document, $\mathrm{Sign}_{k0}(X)$, where $\mathrm{Sign}_{k0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the document, $\mathrm{Sign}_{k0}(X)$ being used to authenticate the document.

26 (Canceled).

27 (Currently Amended). The ~~document~~ check recited in claim ~~26~~ 25, wherein each critical field k of the ~~document~~ check, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k0}(X)$, is covered with another encrypted version of X, $\mathrm{Sign}_k(X)$, where $\mathrm{Sign}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the document.

28 (Currently Amended). The ~~document~~ check recited in claim 27, wherein each critical field k of the ~~document~~ check, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$, is covered with a third encrypted version of X, $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$ which is known to a small group within the institution which issues the document for performing final authentication of the document.

29 (Currently Amended). The ~~document~~ check recited in claim 28, wherein the cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k, are indexed by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $\mathrm{Sign}_k(X)$, $\mathrm{Sign}_{k,0}(X)$, $\mathrm{Sec}_k(X)$ is a family of different cryptographic functions.

30 (Currently Amended). The ~~document~~ check recited in claim 29, wherein the act of adding markings to the ~~document~~ check to transform the ~~document~~ check into a value bearing instrument obscures some of the encryptions, the families of different cryptographic functions preventing cryptographic functions which have been obscured at different places from being used to reconstitute the full cryptographic function.

31 (Canceled).

32 (Currently Amended). The ~~document~~ check recited in claim ~~31~~ 25, wherein the act of adding markings to the check to transform the document into a value bearing instrument obscures some of the encryptions

33 (Canceled).

34 (Currently Amended). The ~~document~~ check recited in claim ~~33~~ 32, wherein each critical field k of the ~~document~~ check, in addition to being

covered by encrypted versions of X, $\text{Sign}_{k0}(X)$, is covered with another encrypted version of X, $\text{Sign}_k(X)$, where $\text{Sign}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\text{Sign}_{k,0}(X)$ which is known to a larger number of authorized banks and institutions for performing an initial authentication of the check.

35 (Currently Amended). The ~~document~~ check recited in claim 34, wherein each critical field k of the ~~document~~ check, in addition to being covered by encrypted versions of X, $\text{Sign}_{k,0}(X)$ and $\text{Sign}_k(X)$, is covered with a third encrypted version of X, $\text{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\text{Sign}_{k,0}(X)$ and $\text{Sign}_k(X)$ which is known to a small group within the bank or institution which issues the check for performing final authentication of the check.

36 (Currently Amended). The ~~document~~ check recited in claim 35, wherein the encrypted function $\text{Sign}_k(X)$ ~~are~~ is communicated to banks and other authorized institutions involved in depositing checks and the encrypted function $\text{Sign}_k(X)$ allows the payee's bank to perform a first authentication of the check.

37 (Currently Amended). The ~~document~~ check recited in claim 36, wherein key $\text{Sign}_{k,0}$ remains the exclusive property of the issuing bank and the encrypted function $\text{Sign}_{k,0}(X)$ is used exclusively by the issuing bank and branches involved in the clearing of checks.

38 (Currently Amended). The ~~document~~ check recited in claim 37, wherein secret key Sec_k is exclusively known to the issuing bank and the encrypted function $\text{Sec}_k(X)$ is used by the issuing bank as a final instrument to verify the check.

39 (New). An apparatus for protecting a check, which will be transformed into a value bearing instrument after adding additional markings to the

check, from fraudulent alteration of the markings comprising:

printing means for printing checks having printed thereon a unique identifier X, the unique identifier including a bank ID, an account ID number and a check number, the check further having critical fields k, k=1,2,3..., the critical fields including a date field, a payee field, amount fields, a payer's field, and an endorser's field, and each critical field k, k=1,2,3..., being covered a large number of lines of fine print comprising encrypted versions ~~a~~ the unique identifier X printed on the document, $\mathrm{Sign}_{k0}(X)$, where $\mathrm{Sign}_{k0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the document;

digitizing means for generating a digitized version of the check in at least selected locations where markings are added to transform the check into a value bearing instrument;

first extracting means for extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sign}_k(X)$, which is known to a large number of authorized institutions; and

first comparing means for comparing a decrypted version of $\mathrm{Sign}_k(X)$ to the unique identifier X as an initial authentication of the document.

40 (New). The apparatus recited in claim 39, wherein each critical field of the check, in addition to being covered by the encrypted version of X, $\mathrm{Sign}_{k,0}(X)$, is covered by another encrypted version of X, $\mathrm{Sign}_k(X)$, where $\mathrm{Sign}_{k0}(X)$ being used to authenticate the document, $\mathrm{Sign}_k(X)$, where $\mathrm{Sign}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the check, further comprising:

second extracting means for extracting from the digitized version of the document the unique identifier X and the corresponding digital encryption of X, $\mathrm{Sign}_{k,0}(X)$, which is known only to an institution that issues the document; and

second comparing means for comparing a decrypted version of $\mathrm{Sign}_{k,0}(X)$ to the unique identifier X as a further authentication of the document.

41 (New). The apparatus of claim 40, wherein each critical field k of the check, in addition to being covered by the encrypted versions of X, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$, is covered with another encrypted version of X, and $\mathrm{Sec}_k(X)$, where $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$ and which is known to a small group within the institution which issues the document for performing final authentication of the check, further comprising:

third extracting means for extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sec}_k(X)$, which is known to a small group within the institution that issues the document; and

third comparing means for comparing a decrypted version of $\mathrm{Sec}_k(X)$ to the unique identifier X as a final authentication of the document.

42 (New). The apparatus of 41, wherein the cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k, are indexed by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic functions $\mathrm{Sign}_k(X)$, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sec}_k(X)$ are families of different cryptographic functions, wherein the families of cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k prevent cryptographic functions which have been obscured at different places by marks added to the check from being used to reconstitute the full cryptographic function.

43 (New). The apparatus recited in claim 41, further comprising one or more secure cryptographic generators (SCGs) for computing the first

family of encrypted functions $\mathrm{Sign}_k(X)$, the second family of encrypted functions $\mathrm{Sign}_{k,0}(X)$, and the third family of encrypted functions $\mathrm{Sec}_k(X)$.

44 (New). The apparatus recited in claim 39, further comprising a database where the unique identifier X and first encrypted function $\mathrm{Sign}_k(X)$ is registered, said database being accessed by the payee's bank to determine whether the check has been previously presented for deposit.